

DOI: 10.7652/xjtuxb201911017

单分类人机检测方法

牛红峰^{1,2}, 朱蓉蓉^{1,2}, 李永明^{1,2}, 丁洁^{1,2}, 蔡忠闽^{1,2}

(1. 西安交通大学智能网络与网络安全教育部重点实验室, 710049, 西安;

2. 西安交通大学电子与信息学部, 710049, 西安)

摘要: 针对人机检测领域中脚本机器人种类多样的问题,提出了一种利用单分类方法基于鼠标行为的人机检测技术,实现对带有行为模拟功能的高级脚本机器人的检测。利用 JavaScript 获取网页页面正常用户的鼠标行为数据,经过数据预处理、特征提取过程获得描述用户行为的特征向量并送入单分类器中,建立人机检测模型。为验证单分类方法的有效性,通过统计分析网页页面正常用户的鼠标行为数据,设计 3 种具有模拟人类功能的脚本机器人,模拟正常用户完成网页页面登录场景任务。使用直线类型的脚本机器人样本参与特征选择,之后提取特征子集,完成单分类器在人机检测领域的性能评价。实验结果表明:单分类器对直线、规则曲线、不规则曲线 3 种脚本机器人检测效果最好的等错误率分别为 7.25%、9.45% 和 12.7%;较二分类方法对未知类型脚本机器人检测效果最好的等错误率为 20.56%;单分类方法具有良好的泛化性。

关键词: 人机检测;脚本机器人;单分类;鼠标行为

中图分类号: TP301.6;TP391.4 **文献标志码:** A **文章编号:** 0253-987X(2019)11-0118-07

Human-Bot Detection with One-Class Classifiers

NIU Hongfeng^{1,2}, ZHU Rongrong^{1,2}, LI Yongming^{1,2}, DING Jie^{1,2}, CAI Zhongmin^{1,2}

(1. Ministry of Education Key Laboratory for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an 710049, China; 2. Faculty of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: A behavior-based human-bot detection technology is proposed to address the problem of a variety of scripted bots in the field of human-bot detection, where one-class classifier is considered to establish a human mouse behavior model to detect sophisticated scripted bots with behavioral simulation functions. JavaScript is installed on the web page to collect the normal users' mouse behaviors, the feature vectors describing the users' behaviors are obtained and sent to the one-class classifiers to construct the human-bot detection model after the data preprocessing and feature extraction process. Statistically analyzing the mouse behaviors of normal users on the web, three types of scripted bots with behavior simulation function are designed to simulate the normal user to complete the task of logging into the web. According to the feature subset selected by the linear scripted bots participated in the feature selection process, the performances of one-class classifiers in human-bot detection are evaluated. Experimental results show that the best equal error rates of one-class classifiers for linear, regular, and irregular curves scripted bots reach 7.25%, 9.45%, and 12.7%, respectively. Compared with two-class method whose best equal error rate is 20.56%, the one-class method is endowed with excellent generalization property for unknown scripted bots detection.

Keywords: human-bot detection; scripted bot; one-class classifier; mouse behavior

收稿日期: 2019-01-18。 作者简介: 牛红峰(1989—),男,博士生;蔡忠闽(通信作者),男,教授,博士生导师。 基金项目: 国家自然科学基金资助项目(61772415)。

网络出版时间: 2019-06-13

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1069.T.20190612.1143.002.html>

人机检测是网络系统分辨人和脚本机器人的技术。脚本机器人是指自动访问和操作信息系统人类操作界面的程序或脚本。脚本机器人是一把双刃剑:一方面,它们能代替人完成枯燥、重复的工作,如搜索引擎通过网络爬虫大规模采集网站信息,建立索引方便人们快速定位到需要的网络资源;另一方面,利用网络机器人可实现拖库、撞库等攻击,给用户的信息、财产等造成极大的安全隐患。更为严重的是,基于脚本机器人的抢票、游戏外挂、刷单等行为破坏了互联网经济的公平性。因此,区分人机的检测技术对互联网生态系统至关重要^[1]。

针对人机检测问题,很多检测方法,如短信验证、邮箱验证、CAPTCHA(俗称“验证码”)^[2]等,被相继提出。由于短信验证的成本较高以及邮箱验证的迟滞性,目前大多数采用基于 CAPTCHA 的方式进行人机检测,常见有的文本输入式、滑动式、点选式等类型。然而,随着人工智能的发展尤其是图像识别技术的发展,通过 CAPTCHA 的方式检测脚本机器人的能力逐渐弱化^[3]。基于 CAPTCHA 原理研制的 reCAPTCHA 是一种具有广泛影响力的人机验证技术,也早在 2017 年被 Brown 等破解^[4]。随着深度学习方法在图像领域的深入应用,快速、高精度地识别 CAPTCHA 成为了可能^[5]。

基于行为的检测技术是人机检测领域的另一个重要方向。Miashima 等通过分析正常用户和游戏机器人在服务器端日志数据中的速度和动作频率等行为模式对游戏机器人进行检测^[6]。Chung 等通过用户的行为相似性来观察和分组用户的游戏行为,为每个玩家群开发了一个本地机器人检测模型^[7]。Kantepe 等提出通过分析推特用户在语义、句法、网络流等方面的行为差异区分机器人账户与正常人类账户^[8]。Chu 等将基于行为的人机检测方法应用于网页端,通过分析不同复杂程度的脚本机器人与正常人的键盘、鼠标等操作行为的差异性,进行人机检测^[9]。van der Walt 等提出利用机器学习的方法对比正常人类与脚本机器人产生的虚假账户的不同^[10]。上述研究利用基于行为的人机检测方法取得了不错的检测效果,验证了基于行为的方法用于人机检测的有效性。然而,以上研究都采用二分类方法进行人机检测。在实际检测中,脚本机器人种类复杂多样,防御方无法获取所有类型的机器人样本数据,因此二分类方法无法对新型未知机器人进行训练、建模。但是,单分类方法能够针对某一类目标样本进行单独建模^[11]、设定目标类边界、区分异

常类与目标类,常用于异常检测^[12]、入侵检测^[13]等样本极度不平衡或者样本较难获取的场景中。

因此,本文提出基于单分类的人机检测方法,通过收集正常用户的鼠标行为数据^[14],建立仅利用正常用户的鼠标行为的人机检测模型。该方法解决了人机检测领域中面对新型机器人层出不穷导致的检测效果不理想的问题,具有较高的泛化能力。

1 单分类人机检测方法

本文提出的基于单分类方法的人机检测模型框架如图 1 所示,包括鼠标行为获取、特征构建及单分类人机检测模型共 3 个模块。

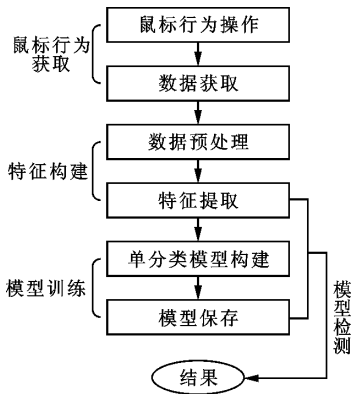


图 1 单分类人机检测框架

1.1 鼠标行为获取

本文以典型的网页登录页面为数据获取场景,将编写好的 JavaScript 内嵌在网页中用于捕获用户操作鼠标时的行为数据。本文设计的登录场景页面如图 2 所示,用户首先通过客户端浏览器打开网页登录页面,然后通过鼠标拖动依次完成输入用户名、密码、验证码、点击登录等操作,完成正常的网页登录。JavaScript 会自动采集上述过程的鼠标行为数据。



图 2 本文设计的登录场景页面

1.2 特征构建

用户在登录页面的操作通常由鼠标和键盘共同组成,鼠标操作被键盘操作分割为多段移动过程。本文将每一段连续的鼠标数据进行单独处理提取相应的特征,得到描述每段鼠标移动的特征向量,将每次登录操作中多段鼠标移动的特征向量求均值,得到描述本次登录鼠标行为的特征向量。

鼠标在移动过程中,内置的 JavaScript 会记录鼠标轨迹时间戳和笛卡儿坐标点,生成 1 组离散的轨迹点坐标与时间戳的集合。鼠标在移动过程中,在屏幕上会形成一段离散轨迹点,如图 3 所示,A、B、C 这 3 个离散点代表鼠标在 3 个不同时刻的坐标点。速度为鼠标在屏幕移动的轨迹长度 $\widehat{AC}$ 与所用时间的比,角度为相邻 3 个轨迹点所形成的角度 $\angle ABC$ 。本文通过分析轨迹点的坐标与时间的关系,提取出描述鼠标行为的 15 个特征,如表 1 所示。

表 1 鼠标行为的特征

特征编号	特征描述
1	相邻 3 个轨迹点的夹角余弦值小于-0.95 的比例
2	前 1/2 轨迹的速度均值与方差之比
3	后 1/2 轨迹的速度均值与方差之比
4	鼠标移动轨迹长度与所用时间之比
5	鼠标移动起始点与终止点之间实际轨迹长度与直线距离之比
6	前 1/4 鼠标轨迹的鼠标移动速度均值
7	后 1/4 鼠标轨迹的鼠标移动速度均值
8	相邻两轨迹点间隔时间的平均值
9	相邻两轨迹点间隔时间的方差
10	相邻两轨迹点距离的平均值
11	轨迹长度与轨迹点数之比
12	相邻 3 个轨迹点夹角余弦值的均值
13	相邻 3 个轨迹点夹角余弦值的标准差
14	相邻 3 个轨迹点夹角余弦值的方差
15	相邻 3 个轨迹点夹角余弦值的均值与方差之比

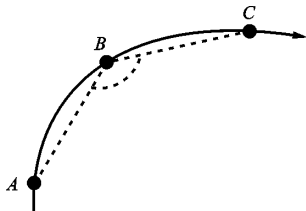


图 3 鼠标轨迹片段

1.3 单分类人机检测模型

该模块包含模型训练与检测两个阶段。

训练阶段:正常用户的鼠标行为样本经过数据预处理及特征提取之后,以特征向量的形式输入单分类器,单分类器利用正常用户样本的特征向量构建单分类检测模型并保存。

检测阶段:该阶段的样本为未知样本,未知样本以特征向量形式输入已训练的检测模型,模型根据设定的阈值判定样本是否属于正常用户。

本文选取模式识别中常用的 4 种单分类器进行人机检测,基本原理如下。

(1)Parzen 窗。Parzen 窗是一种具有坚实理论基础和优秀性能的非参数函数估计方法^[15],该方法利用一组样本中一定范围内各点密度的平均值对总体密度函数进行估计,能够较好地描述一维或多维数据的分布情况。Parzen 窗利用参与训练的正常用户样本来估计描述正常用户样本的特征空间,从而实现对正常用户样本的建模。Parzen 窗有多种核函数,本文采用正态核函数。

(2)支持向量数据描述(SVDD)。SVDD 方法在映射到高维特征空间中找出一个包围目标样本点的超球体,通过最小化超球体的体积让目标样本点尽可能地被包围在超球体中,而非目标样本点尽可能地在超球体外,从而达到两类之间划分的目的^[16]。利用 SVDD 方法能够计算出正常用户样本特征空间的最小超球体中心及半径,从而将超球体之外的样本判定为来自脚本机器人。

(3) k 均值。 k 均值方法假定属于正常用户样本之间的距离相互较近,而正常用户与异常用户样本之间的距离相对较远^[17]。在训练阶段,每 k 个簇的质心被认为是正常用户。在测试阶段,输入的未知样本特征向量到最近质心的欧几里德距离被认为是该样本的分类得分,通过设定不同阈值来判定该样本是来自正常用户还是来自脚本机器人。

(4) k 近邻(knn)。 knn 方法基于新样本与训练集中样本的相似度来建立模型^[18]。在训练阶段,分类器通过计算正常用户样本中两两样本的曼哈顿距离从而建立起正常用户样本的距离矩阵,决定了分类器的分类阈值。在检测阶段,分类器计算未知样本与正常用户每个样本的曼哈顿距离。该样本到最近的前 k 个样本均值被用作 knn 分类器的检测得分。如果该未知样本的得分阈值低于决策得分,那么该样本将会被看成由脚本机器人生成。

2 实验设计

2.1 数据获取

(1)硬件参数。整个实验在相同采集环境下进行,实验设备为 1 台 PC 机,具体参数如下:操作系统为 Windows 7,显示器型号为 HP ModelL 1710,显示器分辨率为 $1\,280\times1\,024$,内存为 2 GB,CPU 型号为 Pentium(R) Dual-Core 3.06 GHz。

(2)数据信息。采集的信息包含一系列鼠标事件标签、运动轨迹的坐标、时间戳、屏幕分辨率、浏览器信息等。

(3)正常用户数据的获取。召集了 30 名在校大学生完成数据采集任务,其中 22 名男生、8 名女生,全部习惯右手操控鼠标,每次采集 5 组数据,连续采集 6 周,每人共采集 30 组数据。

(4)脚本机器人的设计。脚本机器人设计者在针对具有行为防御手段的网页进行脚本机器人攻击时,为逃避服务器对脚本机器人的检测,会尽可能地让脚本机器人模拟正常用户的操作行为。因此,设计者在设计脚本机器人时,需要了解正常用户的操作行为并使脚本机器人产生拟人的操作行为(如鼠标移动、键盘点击等)以规避服务器的检测。

目前,虽有一些可以模拟人类操作行为的公开工具箱(如按键精灵、Auto KeyBoard 等),但并没有公开真正意义上进行人类行为模拟的脚本机器人,更没有相关的公开数据。因此,本文根据脚本机器人相关资料,设计并实现了一种具有一定代表性模拟人类行为的脚本机器人,用于验证本文提出的单分类人机检测方法的实用性和有效性。

正常用户在访问页面时,会产生鼠标移动、键盘点击等基本操作行为,本文在设计脚本机器人时,会最大限度地模拟正常用户在网页端登录场景中的行为。脚本机器人在网页上的操作行为从鼠标移动轨迹形状和速度这 2 方面进行描述。在鼠标移动轨迹方面,设计了直线、规则曲线、不规则曲线共 3 类代表不同复杂程度的轨迹形状,用于验证单分类器对不同类型的脚本机器人均具有良好的检测性能。选取抛物线形状作为规则曲线轨迹的代表,利用计算机图形学中的贝塞尔曲线^[19]生成方法实现上述 3 种轨迹形状。在鼠标移动速度方面,通过计算 30 人的鼠标移动速度统计属性,设计产生 3 种不同速度:恒定速度,符合均匀分布的速度,符合高斯分布的速度。本文设计的 3 类共 9 种脚本机器人的属性如表 2 所示,每类脚本机器人分别产生 300 个样本。

表 2 3 类共 9 种脚本机器人的属性

脚本机器人编号	鼠标移动轨迹形状	鼠标移动速度
1	直线	恒定
2	直线	均匀分布
3	直线	高斯分布
4	规则曲线	恒定
5	规则曲线	均匀分布
6	规则曲线	高斯分布
7	不规则曲线	恒定
8	不规则曲线	均匀分布
9	不规则曲线	高斯分布

2.2 特征选择

区分性较差的特征和冗余特征会对模型产生较大影响,导致训练时间浪费及分类模型复杂。此外,直接使用全部特征集会导致建模过程中产生过拟合等问题,从而降低模型的泛化性能。因此,本文剔除对分类模型贡献较少的特征,保留性能较好的特征子集,利用筛选出的特征子集进行模型的训练,从而提高模型的泛化能力。

本文采用机器学习中广泛用于特征选择的 Fisher Score 方法^[20]进行特征选择,具体过程如下:

(1)从正常用户样本和直线脚本机器人样本中随机抽取等量样本并以特征向量的形式保存;

(2)为正常用户样本与直线脚本机器人样本分别标注为 1 和 0;

(3)将标注好的特征向量送入 Fisher Score 特征选择器;

(4)特征选择器输出各特征的 Fisher Score,用 S_{Fisher} 表示。

表 3 为 15 个特征的 S_{Fisher} ,得分越高表明特征区分度越明显,可以看出:自编号 15 开始的 8 个特征的得分较低且趋于稳定,因此选出编号为 1、2、11、6、7、12、5 共 7 个具有较高得分的特征进行实验。

表 3 15 个特征的 S_{Fisher}

特征编号	S_{Fisher}	特征编号	S_{Fisher}
1	2.277	3	0.016
2	1.052	9	0.012
11	0.809	4	0.010
6	0.452	13	0.007
7	0.217	14	0.005
12	0.201	10	0.002
5	0.166	8	0.001
15	0.035		

2.3 训练及测试过程

收集 30 人的数据为正样本,脚本机器人在登录时产生的数据为负样本。训练阶段选取一定数量的正样本作为训练集,为每种单分类器创建正常用户检测模型。测试阶段分别选用剩余正样本与负本来测试检测模型。

为了实验公平性,正常用户的测试样本和训练样本由不同用户群产生。为降低随机因素对实验的影响,每种实验进行 500 次,取均值作为实验结果。

2.4 性能评价指标

误识率表示脚本机器人样本被误认为正常用户样本的数量占测试集中所有脚本机器人样本的比例。拒识率表示正常用户样本被误认为脚本机器人样本的数量占测试集中所有的正常样本的比例。等错误率 R_{EE} 表示误识率与拒识率相等时的错误率,本文采用 R_{EE} 作为评估模型检测性能的指标。

3 实验结果分析

3.1 单分类器的性能分析

本实验对比分析 4 种常见单分类器在人机检测方面的性能。采用 10 折交叉验证的方法,随机抽取 27 人,得到共 27×30 个样本数据进行训练,选取剩余 3 人共 3×30 个样本数据用于测试。为保证测试集内正常用户样本与脚本机器人样本平衡,从每类脚本机器人中,随机选取 90 个样本参与测试。表 4 呈现了 4 种分类器分别利用 7 个特征与 15 个特征进行检测时的 R_{EE} 。

表 4 单分类器对不同类型脚本机器人检测的 R_{EE}

分类器	特征数量	$R_{EE}/\%$		
		直线	规则曲线	不规则曲线
Parzen 窗	7	8.03	11.11	16.20
	15	10.08	12.39	18.23
SVDD	7	7.25	9.45	12.70
	15	15.88	18.70	23.80
k 均值	7	11.81	14.94	19.74
	15	20.53	21.25	28.37
knn	7	10.26	12.86	16.55
	15	12.98	15.44	20.04

注:表中加粗数据为最优值。

从表 4 可以得出:单分类器对脚本机器人检测效果最好时 R_{EE} 为 7.25%、最差时为 28.37%,能够实现对脚本机器人的有效检测;利用经过特征选择后的特征子集参与检测,检测性能从高到低的分类

器依次为 SVDD、Parzen 窗、 knn 、 k 均值;利用全部 15 种特征参与检测,检测性能从高到低的分类器依次为 Parzen 窗、SVDD、 knn 、 k 均值;SVDD 与 Parzen 窗在不同的特征集中均表现出较好的检测性能;随曲线轨迹复杂程度的提高,单分类器的检测效果逐渐降低;相较于使用全部 15 种特征,采用经过特征选择之后得出的 7 种特征子集进行检测时,单分类器的性能有较大的提升,如 SVDD 对直线类型脚本机器人检测时, R_{EE} 从 15.88%降低至 7.25%,证明了特征选择的有效性。

3.2 训练规模对单分类器性能的影响

为探索训练样本规模对单分类人机检测方法的影响,选取 3.1 节实验中检测性能最好的 SVDD 和 Parzen 窗这 2 种单分类器,利用经特征选择后的特征子集进行检测。随机选取 3 人的全部样本作为测试集,根据测试集中正常用户样本的数量,随机从不同类型脚本机器人样本中抽取等量的测试样本,使测试集中正常用户样本和脚本机器人样本的数量始终保持平衡。训练集从除测试集以外的 27 人中抽取,本实验依次随机选取 9、12、15、18、21、24、27 人的全部样本作为训练集,分析训练集增加过程中检测效果的变化。表 5 为不同训练规模下 2 种分类器对 3 种不同复杂程度的脚本机器人检测结果。

表 5 不同训练规模下人机检测的 R_{EE}

训练集人数	分类器	$R_{EE}/\%$		
		直线	规则曲线	不规则曲线
9	Parzen 窗	9.75	12.59	17.77
	SVDD	7.99	10.42	13.90
12	Parzen 窗	9.20	12.16	17.37
	SVDD	7.64	10.05	13.45
15	Parzen 窗	9.04	11.94	17.07
	SVDD	7.62	9.92	13.30
18	Parzen 窗	8.65	11.70	16.63
	SVDD	7.45	9.87	13.17
21	Parzen 窗	8.56	11.48	16.46
	SVDD	7.35	9.71	13.01
24	Parzen 窗	8.28	11.33	16.35
	SVDD	7.29	9.61	12.85
27	Parzen 窗	8.10	11.15	16.19
	SVDD	7.25	9.45	12.69

注:表中加粗数据为最优值。

从表 5 可以看出,随着训练样本规模的增大,无论检测何种类型的脚本机器人,2 种分类器的检测

性能均越来越好,即 R_{EE} 随着训练规模的增大逐渐降低。以 SVDD 分类器为例,在对直线轨迹的脚本机器人检测时,随着训练规模从 9 人增至 27 人,检测的 R_{EE} 从 7.99% 逐渐降至 7.25%。这是因为更多的训练样本能够使单分类器更全面地针对目标类样本进行建模,得到更好的检测模型,从而能更好地区分正常用户和脚本机器人。此外,在对同种类型脚本机器人检测时,SVDD 分类器均优于 Parzen 窗分类器,推测是因为 SVDD 分类器可以弥补先验知识的不足,将分类问题转化为二次优化问题,使其仍然能保持相对较高的准确性^[21]。

3.3 与二分类器的性能对比

为进一步说明单分类方法的有效性,与经典的二分类方法支持向量机(SVM)和 knn 进行比较实验。在对已知类型的脚本机器人检测时,部分正常用户参与训练,剩余的正常用户样本参与测试,参与训练和检测的机器人样本来自同种类型的脚本机器人。在对未知类型的脚本机器人检测时,训练样本为部分正常用户样本和某类脚本机器人样本,测试样本为剩余正常用户样本和异于训练集中机器人类型的脚本机器人样本。利用经过特征选择后的 7 个特征参与实验,具体结果如表 6 和表 7 所示。

表 6 二分类器对已知类型脚本机器人检测的 R_{EE}

训练集	测试集	$R_{EE}/\%$	
		SVM	knn
直线	直线	0.43	0
规则曲线	规则曲线	0.70	0.14
不规则曲线	不规则曲线	1.20	0.20

表 7 二分类器对未知类型脚本机器人检测的 R_{EE}

训练集	测试集	$R_{EE}/\%$	
		SVM	knn
直线	规则曲线	22.90	29.70
	不规则曲线	23.09	29.89
规则曲线	直线	22.12	20.56
	不规则曲线	25.53	20.66
不规则曲线	直线	23.00	36.19
	规则曲线	30.22	36.72

注:表中加粗数据为最优值。

分析表 6 和表 7 可得:二分类器对已知类型脚本机器人具有较好的检测效果,但对未知类型脚本机器人的检测效果大幅下降;SVM 和 knn 这 2 种二分类器对未知类型脚本机器人检测效果最好的 R_{EE}

仅为 22.12%、20.56%,而在第 3.1 节的实验中,单分类器对未知类型的规则曲线和非规则曲线脚本机器人检测效果最好的 R_{EE} 分别为 9.45%、12.70%。由此得出:二分类器建立针对已知类型脚本机器人的检测模型,适用于对已知类型脚本机器人的检测,对未知类型脚本机器人会出现较大的检测误差,可泛化能力较弱;单分类器基于正常用户样本建立人机检测模型,不用考虑脚本机器人类型的改变,可泛化能力较强。

4 结 论

本文提出一种基于行为的人机检测技术,采用单分类方法建立人的鼠标行为模型,实现对带有行为模拟功能高级脚本机器人的检测。以网页端登录场景中的鼠标行为为研究对象,仅利用正常用户鼠标行为数据,建立基于单分类方法的人机检测模型,实现对 3 种不同复杂程度轨迹的脚本机器人的检测。实验结果表明:经过特征选择之后,性能表现最好的 SVDD 单分类器对直线类型脚本机器人检测的 R_{EE} 为 7.25%,单分类方法的可行性得到了验证;单分类器的检测性能随着训练规模的增大而提升,当训练人数为 9 时,SVDD 分类器对直线类型脚本机器人检测的 R_{EE} 为 7.99%,当训练人数为 27 时, R_{EE} 为 7.25%; knn 与 SVM 这 2 种二分类器在面对未知类型脚本机器人时,检测性能表现最好的为 knn 基于规则曲线脚本机器人建立的检测模型对直线类型脚本机器人的检测,此时 R_{EE} 为 20.56%,但仍大大低于本文所用单分类器对未知类型脚本机器人的检测性能;单分类方法在面对新型未知样本脚本机器人时展示了较强的泛化性。

由于在实际场景中脚本机器人类型复杂多变、未知性强,因此本文提出的人机检测方法具有较强实际应用意义,可为人机检测提供一种新的思路。

参考文献:

[1] UZUN E, CHUNG S P H, ESSA I, et al. rtCaptcha: a real-time captcha based liveness detection system [EB/OL]. [2019-01-10]. https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_01B-4_Uzun_paper.pdf.
[2] VON AHN L, BLUM M, HOPPER N J, et al. CAPTCHA: using hard AI problems for security [M]// Lecture Notes in Computer Science: Vol. 2656. Berlin, Germany: Springer Verlag, 2003: 294-311.
[3] YE G X, TANG Z Y, FANG D Y, et al. Yet another

- text captcha solver [C] // Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York, NY, USA: ACM, 2018: 332-348.
- [4] BROWN S S, DIBARI N, BHATIA S. I am 'totally' human: bypassing the reCaptcha [C] // 2017 13th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS). Piscataway, NJ, USA: IEEE, 2017: 9-12.
- [5] TANG M Y, GAO H C, ZHANG Y, et al. Research on deep learning techniques in breaking text-based captchas and designing image-based captcha [J]. IEEE Transactions on Information Forensics and Security, 2018, 13(10): 2522-2537.
- [6] MISHIMA Y, FUKUDA K, ESAKI H. An analysis of players and bots behaviors in MMORPG [C] // IEEE International Conference on Advanced Information Networking & Applications. Piscataway, NJ, USA: IEEE, 2013: 870-876.
- [7] CHUNG Y, PARK C Y, KIM N R, et al. A behavior analysis-based game bot detection approach considering various play styles[J/OL]. ETRI Journal, 2013, 35(6): 1058-1067. [2018-11-15]. <https://arxiv.org/abs/1509.02458>.
- [8] KANTEPE M, GANIZ M C. Preprocessing framework for twitter bot detection [C] // 2017 International Conference on Computer Science and Engineering (UBMK). Piscataway, NJ, USA: IEEE, 2017: 630-634.
- [9] CHU Z, GIANVECCHIO S, WANG H N. Bot or human? a behavior-based online bot detection system [M] // Lecture Notes in Computer Science: Vol. 11170. Berlin, Germany: Springer International Publishing, 2018: 432-449.
- [10] VAN DER WALT E, ELOFF J. Using machine learning to detect fake identities: bots vs humans [J]. IEEE Access, 2018, 6: 6540-6549.
- [11] TAX D M J. One-class classification: concept-learning in the absence of counter-examples [D]. Delft, Netherlands: Delft University of Technology, 2001: 1.
- [12] CHANDOLA V, BANERJEE A, KUMAR V. Anomaly detection [J]. ACM Computing Surveys, 2009, 41(3): 1-58.
- [13] ZAINAL A, MAAROF M A, SHAMSUDDIN S M, et al. Ensemble of one-class classifiers for network intrusion detection system [C] // 2008 the Fourth International Conference on Information Assurance and Security. Piscataway, NJ, USA: IEEE, 2008: 180-185.
- [14] 房超, 蔡忠闽, 沈超, 等. 基于鼠标动力学模型的用户身份认证与监控 [J]. 西安交通大学学报, 2008, 42(10): 1235-1239.
- FANG Chao, CAI Zhongmin, SHEN Chao, et al. Authentication and monitoring of user identities based on mouse dynamics [J]. Journal of Xi'an Jiaotong University, 2008, 42(10): 1235-1239.
- [15] PAN Z W, XIANG D H, XIAO Q W, et al. Parzen windows for multi-class classification [J]. Journal of Complexity, 2008, 24(5/6): 606-618.
- [16] PARK J, KANG D, KIM J, et al. SVDD-based pattern denoising [J]. Neural Computation, 2007, 19(7): 1919-1938.
- [17] WONG M A. Asymptotic properties of univariate sample k -means clusters [J]. Journal of Classification, 1984, 1(1): 255-270.
- [18] SHEN C, CAI Z M, GUAN X H, et al. On the effectiveness and applicability of mouse dynamics biometric for static authentication: a benchmark study [C] // 2012 5th IAPR International Conference on Biometrics (ICB). Piscataway, NJ, USA: IEEE, 2012: 378-383.
- [19] WANG S, CHEN L, HU H S, et al. Doorway passing of an intelligent wheelchair by dynamically generating Bézier curve trajectory [C] // 2012 IEEE International Conference on Robotics and Biomimetics (ROBIO). Piscataway, NJ, USA: IEEE, 2012: 1206-1211.
- [20] WANG S, LIU C L, ZHENG L. Feature selection by combining fisher criterion and principal feature analysis [C] // 2007 International Conference on Machine Learning and Cybernetics. Piscataway, NJ, USA: IEEE, 2007: 1149-1154.
- [21] SHEN C, CAI Z M, GUAN X H, et al. Performance evaluation of anomaly-detection algorithms for mouse dynamics [J]. Computers & Security, 2014, 45: 156-171.

(编辑 陶晴)